PCoIP Connection Manager and Security Gateway Administrators' Guide

25.03

Table of contents

Overview

Connection Manager and Security Gateway

The *Connection Manager* and the *Security Gateway* are components of HP Anyware, and can be deployed together as a set or individually. Multiple instances of the Connection Manager and/or the Security Gateway can be deployed to handle mixed LAN and WAN access points, enable security gateway failover, or for scaling large systems.

Components in this release

The Connection Manager and Security Gateway 25.03 is a combined release containing:

- Connection Manager 25.03
- Security Gateway 23.04

About the Connection Manager

The *Connection Manager* enables connections between Anyware clients and Anyware agents installed on remote desktops. It uses a required third-party connection broker to authenticate users, query available desktops and applications, and then establish a PCoIP connection between the client and the selected desktop.

About the Security Gateway

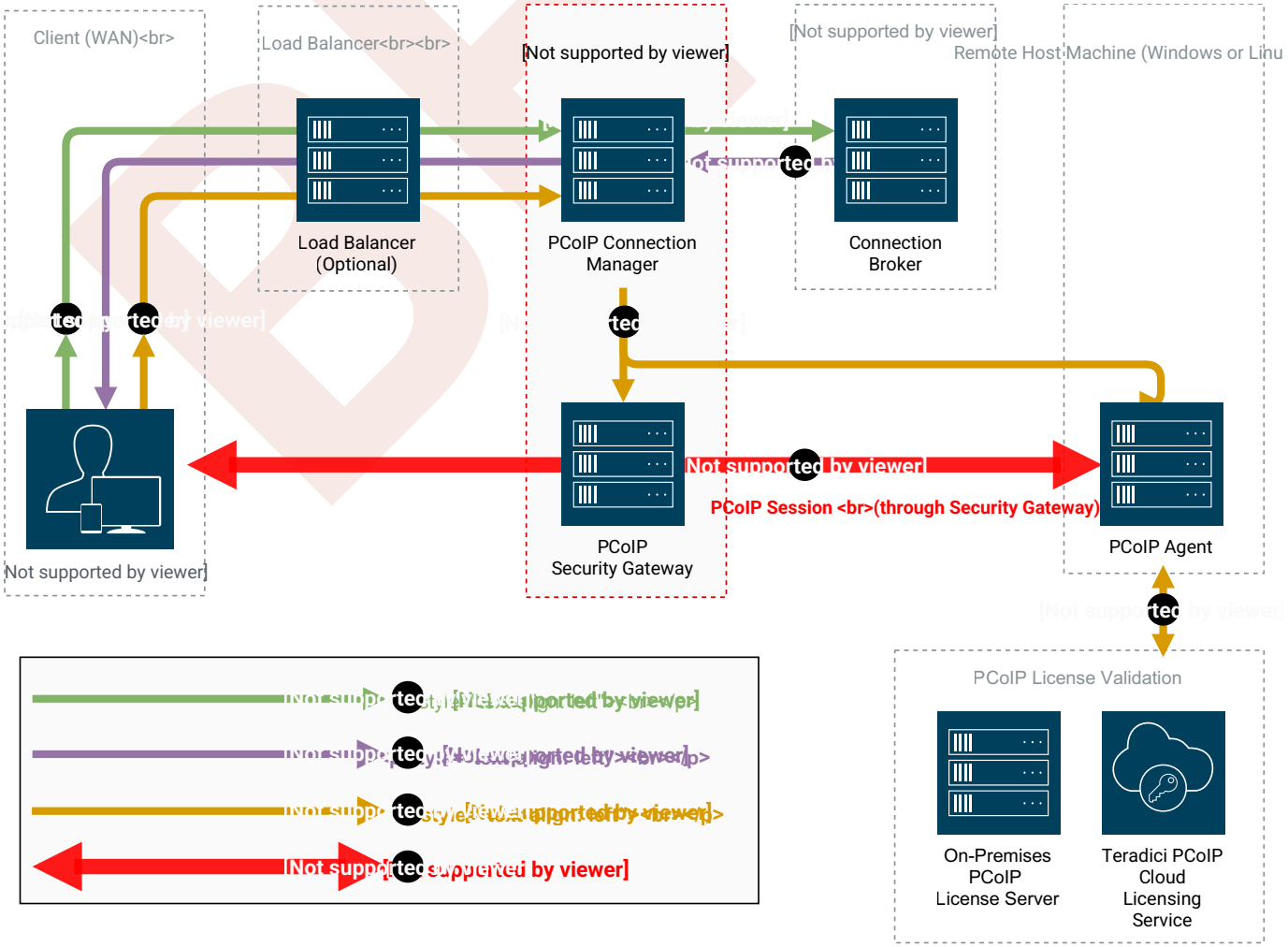
The *Security Gateway* enables WAN users to securely access their remote desktops via the Internet without a VPN connection. You can optionally deploy multiple Security Gateways so that if the gateway being used by a PCoIP session becomes unavailable, the session is automatically transferred to the next available gateway. To use this feature, configure the Connection Manager using the `--external-sg-ip` flag with the addresses of the failover security brokers.

Note

The Security Gateway is not required for LAN access.

Establishing a PCoIP Connection With the Connection Manager and Security Gateway

The diagram shown next illustrates a brokered connection to the Anyware host machine using the Connection Manager and the Security Gateway.



> **Caution: A dedicated server is strongly recommended**
>
> Since the Connection Manager is a component that handles authentication data for users connecting to virtual desktops, we strongly recommend installing the Connection Manager and Security Gateway on a dedicated server that is accessible only by authorized system administrators according to your organization's security policy.

Deployment Scenarios

Depending on your deployment scenario, you can install the Connection Manager with the Security Gateway disabled.

- **All your desktops are on a LAN (internal access only)**: you may only need to install one Connection Manager. Since a Security Gateway isn't required for LAN connections, you can optionally disable it.
- **All your desktops are on a WAN**: Install one Connection Manager, and enabling one or more Security Gateways. The Connection Manager handles PCoIP Connection establishment and the Security Gateway(s) secures the PCoIP session across the public internet.
- **Your desktops are on both a LAN and WAN**: We recommend installing at least two groups of connection managers; one for internal access with the Security Gateway disabled, and one for external access with one or more Security Gateway(s) enabled. You can set up the DNS so that internal and external users are routed to the appropriate connection manager.
- **If you are exceeding the system specifications or have high availability requirements**: If you serve a large number of desktops, or require high availability, install additional connection managers and implement load balancing.

What's New in This Release

Release 25.03 of the Connection Manager and Security Gateway includes bug fixes, security enhancements, and the following updates:

This content is currently being developed.

System Requirements

The minimum system requirements for a Connection Manager and Security Gateway are:

- 2 or more CPUs or vCPUs, 2.5 GHz or higher
- 4 GB of RAM
- 4 GB of swap space
- 10 GB of free disk space in var directory

Supported operating systems:

- RHEL 8
- RHEL 9
- Rocky Linux 8
- Rocky Linux 9

If the connection broker is configured to identify resources by host name, then DNS must be available in Connection Manager and the PCoIP Broker.

Installation Prerequisites

The Connection Manager and Security Gateway depends on the following packages:

- **Docker 20.10.0** or higher

Install or update OpenSSL version to **OpenSSL 3.0** or higher.

Project dependencies must be installed on the production machine *before* installing the Connection Manager and Security Gateway.

> ⚠ **Caution: Dependencies in offline environments**
>
> If your deployment will be running in an environment that is not connected to the public internet (a *dark site*), you must download the package dependencies, transfer them to the production machine, and install them before installing the Connection Manager and Security Gateway.

Open SSL Minimum Requirements

The following procedures use openssl to create and manage certificates. If you use another tool, adapt these instructions accordingly. The minimum Open SSL version on your virtual machine is 3.0.

Connection Manager and Security Gateway Performance Limits

The following statistics represent the performance limits of the Connection Manager and Security Gateway with a *minimum* system configuration. You can exceed these limits, unless indicated, with more powerful systems.

Connection Manager Limits

Session Establishment Limits

Based on the minimum connection manager system requirements, the Connection Manager can establish the following number of sessions:

- 40 simultaneous *in-process* session establishment sequences
- Up to 400 simultaneous client communications

Security Gateway Limits

Session Limits

Each Security Gateway supports a maximum of **5,000** simultaneous sessions. You can lower this limit by changing the `MaxConnections` setting in `/opt/teradici/pcoipcm_data/data/SecurityGateway.conf`. If you need to support more than 5,000 simultaneous sessions, deploy additional Connection Manager and Security Gateways behind a load balancer.

Bandwidth Limits

When using the Connection Manager and Security Gateway there are certain session establishment and session bandwidth limits when dealing with external connections.

The following table outlines the RAM, vCPU and correlated estimated bandwidth support for all combined concurrent sessions:

vCPUs	RAM	Estimated Bandwidth
2vCPU	7.5 GB RAM	~ 365 Mbit/s
4vCPU	15 GB RAM	~ 830 Mbit/s
8vCPU	30 GB RAM	~ 1100 Mbit/s

Estimated Bandwidth

These are estimated bandwidth levels. The bandwidth can vary based on the host, OS, CSP, etc.

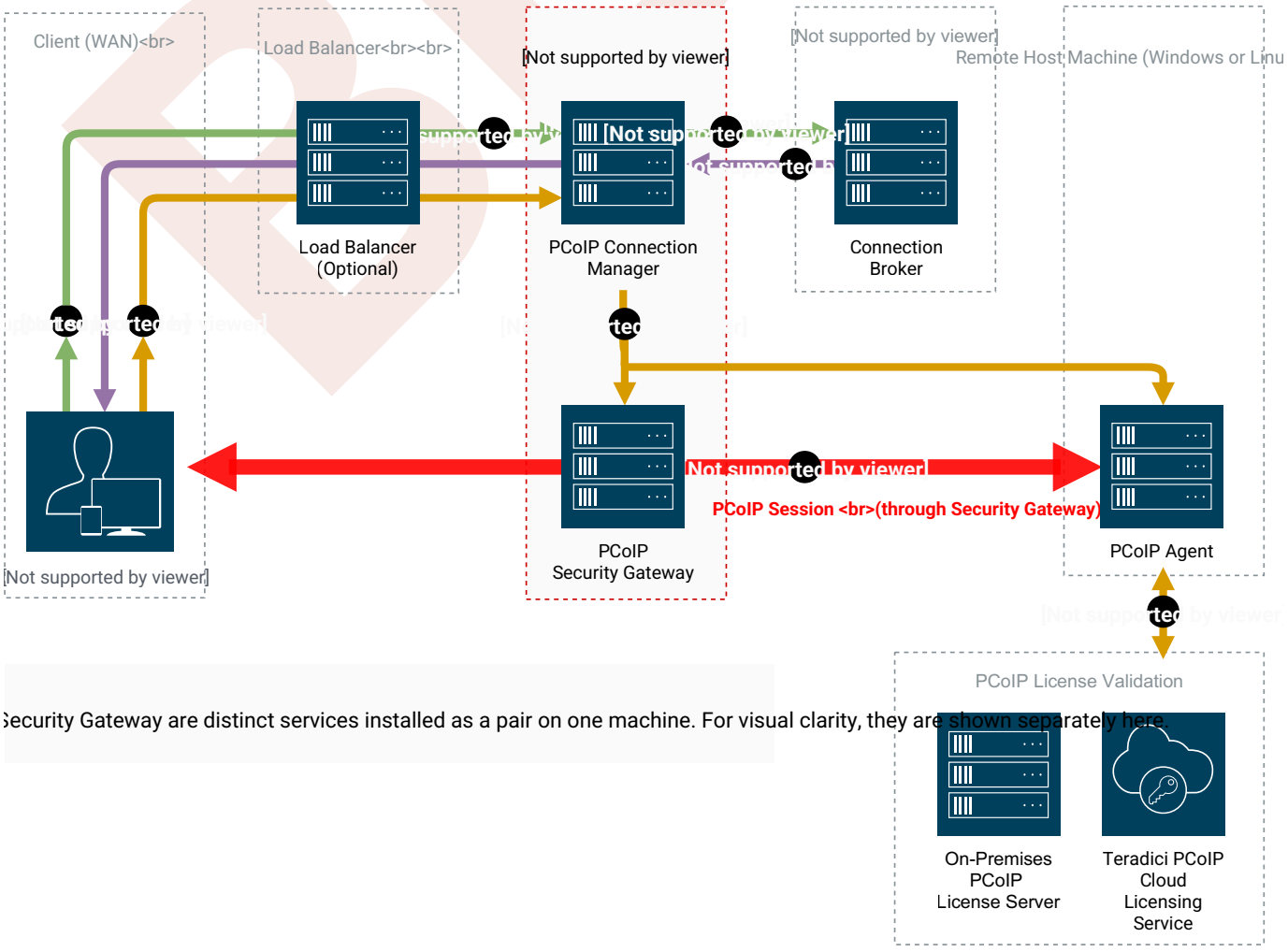
1100 Mbit/s is approximately the maximum bandwidth that can be achieved. Additional gains may be possible with larger sizing.

System Planning

Before deploying the Connection Manager and Security Gateway, ensure you understand the PCoIP session establishment process and how load balancers and firewalls fit in.

Session Establishment

Here's the sequence of events involved in establishing a PCoIP session in a typical brokered scenario. In this example, the Anyware client is outside the firewall, so the Security Gateway is enabled to secure the connection and to proxy authorized traffic.



ecurity Gateway are distinct services installed as a pair on one machine. For visual clarity, they are shown separately here.

1. A user provides a server name and address to their Anyware client, which passes the data to the **Connection Manager** (this can be relayed through a load balancer, as shown here).

2. The *Connection Manager* communicates with the **Connection Broker** to authenticate the user and to obtain the list of desktops the user is entitled to use.
3. The *Connection Broker* passes the list of desktops back to the the **Anyware Client**.
4. The user selects a desktop from the client UI, and their choice is passed back to the **Connection Manager**.
5. The *Connection Manager* prepares the **Security Gateway** and the requested desktop's **Anyware Agent**.
6. The **Anyware Agent** acquires a session license from a licensing service (either the **PCoIP Cloud Licensing Service** or the a local **License Server**).
7. The PCoIP session is established. The **Anyware Client** now communicates directly with the selected desktop using the PCoIP Protocol.

> **Note: Security Gateway in LAN systems**
>
> The Security Gateway secures PCoIP communications through the firewall. In systems where Anyware clients are on the WAN, PCoIP traffic is relayed through the Security Gateway. When the entire PCoIP system is on your company LAN, the Security Gateway is unnecessary and the Anyware Client and Anyware agent communicate directly.

Load Balancing

You can use load balancers in front of multiple connection managers and security gateways to distribute system load to optimize performance. The load balancer must support the following:

- HTTPS
- Sticky sessions by the jsessionid

During session establishment, the Connection Manager retrieves the public IP addresses of the Security Gateways and passes them to the client. After the session is established, the client uses a provided IP address to communicate directly with a Security Gateway.

Important: The Security Gateway's public IP address must be set during installation

When a Security Gateway is installed using the `--enable-security-gateway` flag, its public IP address is set using the `--external-pcoip-ip` flag during installation.

If the public IP address is configured to point to the *load balancer* instead of the **Security Gateway**, the load balancer may direct the client to a Security Gateway on the wrong server. If this happens, the client will not be able to establish a session.

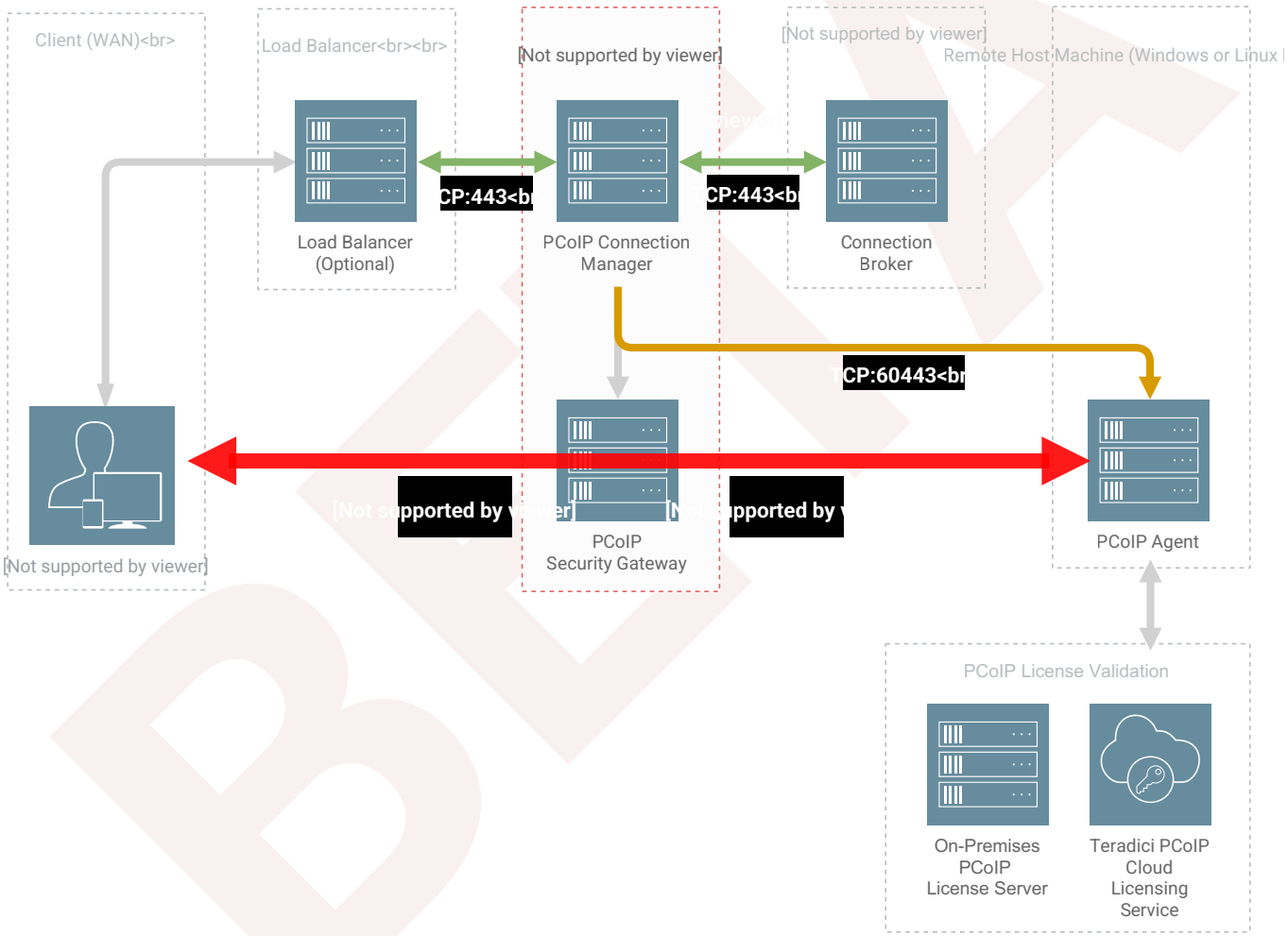
Public IP Address

The machine(s) with a Connection Manager and/or a Security Gateway on it must have a public IP address if it is directly accessed from WAN.

To see how load balancers fit into firewall configurations, refer to Configuring Firewalls.

Configuring Firewalls

If there is a firewall on the Connection Manager server, ensure ports for PCoIP traffic are open so that users can access their desktop. The illustration shown next shows the default port numbers.



Firewall recommendations for establishing a PCoIP Session

Source	Port	Destination	Port	Description
Anyware Client	*	Connection Manager	TCP: 443	PCoIP broker protocol (HTTPS)
Connection Manager	*	Connection broker	TCP: 443	PCoIP broker protocol (HTTPS)
Connection Manager	*	Anyware Agent	TCP: 60443	Anyware agent protocol
Anyware Client	*	Security Gateway	UDP: 4172	PCoIP user data
PCoIP Client	*	Security Gateway	TCP: 4172	PCoIP control information
Security Gateway	*	Anyware Agent	TCP: 4172	PCoIP control information
Security Gateway	UDP: 55000	Anyware Agent	UDP: 4172	PCoIP user data. *When deploying a desktop with an Anyware agent, only port 4172 needs to be open.*

Inbound Connections

Ensure these ports are open for inbound connections:

Port	Purpose
443 TCP	Used by clients to connect to the Connection Manager
4172 TCP/UDP	Used by authorized clients to connect to the Security Gateway

Instructions for opening these ports are included in the installation procedures.

Note that RHEL 8 and Rocky Linux 8 permit all outbound traffic by default.

Important: Other required services may need open outbound ports

If the Connection Manager is on a network behind a firewall that blocks outbound connections, ensure that the required ports for other required operating system services are open. We recommend that DHCP, DNS, and NTP are active for Connection Manager operation.

Configuring Docker Network

The default docker network environment for the Connection Manager and the Security Gateway is assigned to `10.101.0.0/24`.

If your company network CIDR overlaps `10.101.0.0/24`, please use option --docker-network-cidr to provide a new network CIDR for docker during installation / updating. Addresses from any of the following CIDR classes can be used:

```
Class A: 10.0.0.0 to 10.255.255.255.
Class B: 172.16.0.0 to 172.31.255.255.
Class C: 192.168.0.0 to 192.168.255.255.
```

for example: pcoip-cmsg-setup install --docker-network-cidr 172.16.0.0/24

Installing

Installing the Connection Manager and Security Gateway

The following sections outline how to install the Connection Manager and Security Gateway.

Before You Begin

Before you proceed with installation, note the following:

- **Docker must be installed** before you begin. For instructions, see About Docker.
- Make sure ports TCP:80, TCP:443, TCP:4172, and UDP:4172 are open:

```
sudo firewall-cmd  --add-port 80/tcp
sudo firewall-cmd  --add-port 443/tcp
sudo firewall-cmd  --add-port 4172/tcp
sudo firewall-cmd  --add-port 4172/udp
```

- If you will be using IPv6, set up the required port forwarding rules:

```
# Add port forwarding rules
sudo firewall-cmd  --add-forward-port=port=443:proto=tcp:toport=8443
sudo firewall-cmd  --add-forward-port=port=80:proto=tcp:toport=8080
sudo firewall-cmd  --add-rich-rule='rule family=ipv6 forward-port
protocol=tcp port=443 to-port=8443'
sudo firewall-cmd  --add-rich-rule='rule family=ipv6 forward-port
protocol=tcp port=80  to-port=8080'

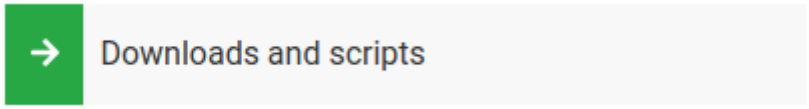
# Make the new settings persistent
sudo firewall-cmd --runtime-to-permanent
```

- If your environment has `podman` or `buildah` installed, uninstall them before proceeding.

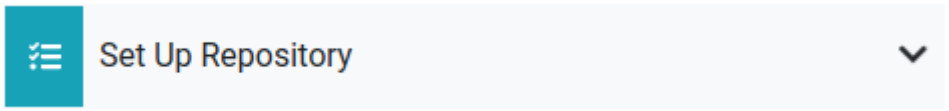
```
sudo dnf erase podman buildah -y
```

Install Modern Connection Manager and Security Gateway

1. On the machine that hosts the Connection Manager and/or the Security Gateway, open a browser and go to the Connection Manager and Security Gateway download page.
2. Click **Downloads and scripts**:

   If you see a login button instead, click it to log into the site and then proceed.
3. Accept the End User License Agreement, then click **Set Up Repository**:

   The window expands and show the setup scripts for each supported operating system. Copy the command for your system to the clipboard.
4. Open a console window and paste in the command you copied in the previous step. You may need to press `Enter` to execute it.

   The command fetches a configuration script from our servers and runs it locally, setting up and configuring the repository on the local machine.
5. Install the Connection Manager and Security Gateway package:

   ```
   sudo dnf install pcoip-cmsg-setup
   ```

6. After the package is installed locally, run the `pcoip-cmsg-setup install` command with the required flags to complete installation.

   ```
   sudo pcoip-cmsg-setup install <installation_flags>
   ```

   There are a number of options and settings available. You can invoke the `install` command with the `--help` flag to list them:

   ```
   ```text
   pcoip-cmsg-setup install --help
   ```
   ```

   They are also listed in the next section.

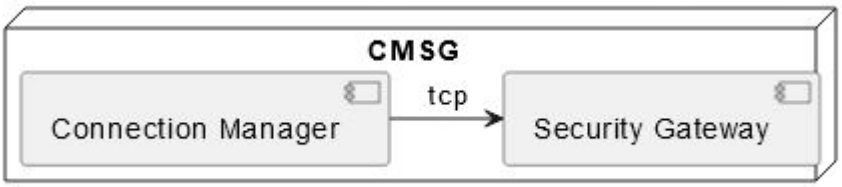
The `install` command prompts you for required parameters that have not been supplied via flags.

Installing Components Individually

- To install only the Connection Manager use `--enable-security-gateway=false`.
- To install only the Security Gateway use `--enable-connection-manager=false`.
- Otherwise both the Connection Manager and Security Gateway are installed by default.

Deployment Scenarios

- Connection Manager and Security Gateway deployed together: This is the default option when installing. There is no gateway failover in this deployment.



- Connection Manager and Security Gateways deployed separately: There is gateway failover in this scenario.

- Connection Manager and Security Gateways deployed together and separately: There is gateway failover in this scenario.

Installation Flags and Options

The following flags can be used to provide values at the command line. Flags that are required are identified in the description.

Boolean values should be provided as either `true` or `false`, lowercased, as in this example:

```
--example-flag=true
```

Flag	Type	Description
`--accept-policies`	Boolean	Automatically accepts the EULA and Privacy Policy. **Required.**
`--broker-url`	String	The URL of the PCoIP Broker, specified either as a https://: or https://: or https://[]:. **Required**.
`--ca-cert`	String	The full path and filename of the custom Certificate Authority's public certificate to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--compose-file`	String	Specify the full path to a local docker-compose file.
`--darksite-bundle-path`	string	The path of darksite install bundle to be used for darksite installation
`--docker-password`	String	Password to login to private registry.
`--docker-registry`	String	Specifies the HP source for Anyware Connector images to be install from. **Debugging only**: This is intended to be used for debugging purposes and should not be used without guidance from HP support. Using this flag incorrectly can result in failed installations.
`--docker-username`	String	Username to login to private registry.
`--enable-collaboration`	Boolean	Allow multiple Anyware clients to collaborate on a Anyware agent. (Default=true)
`--enable-ipv6`	Boolean	Enables IPv6 connections (Default=false). To enable IPv6 use `--enable-ipv6=true`. To disable IPv6 use `--enable-ipv6=false`, or omit this flag.
`--external-pcoip-ip`	StringArray	Sets the public IP address of Security Gateway. If `--enable-ipv6` is true, this option may be used twice (once for IPv4 and once

Flag	Type	Description
		for IPv6). **Required if Security Gateway is enabled**
`--enable-security-gateway`	Boolean	Enable and use the Security Gateway (Default=true).
`--help`		Lists all available flags.
`--host-address`	stringArray	Sets the host FQDN/IP address. The option may be used twice (once for the IP address and once for the FQDN)
`--ignore-disk-req`	Boolean	Ignore the check for the minimum disk space requirement.
`--license-server-url`	String	The address of the locally installed License Server. Example: `https://<license-server-address>:<port>`
`--self-signed`	Boolean	Automatically generate self-signed SSL cert and key for testing purposes. If specified, `--ssl-key` and `--ssl-cert` options are ignored.
`--ssl-cert`	String	The full path and filename of the SSL certificate to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--ssl-key`	String	The full path and filename of the SSL key to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--docker-network-cidr`	Sets CIDR for Connection Manager's docker network for services. If default docker network IP range is conflict with intranet, this option should be used to solve the confliction	
`--debug`	String	Sets the log verbosity higher to help with debugging installation issues.

Flag	Type	Description
`--enable-connection-manager`	Boolean	Enable and use the Connection Manager (Default=true).
`--external-sg-ip`	StringArray	Sets public IP addresses of external Security Gateways to enable gateway failover if a Security Gateway becomes unavailable. **Only IP addresses are supported**. IP addresses should be provided in the format `--external-sg-ip=ipAddr1 --external-sg-ip=ipAddr2...`
`--jwt-verifying-cert`	String	The full path and filename of the certificate that the Security Gateway should use to validate the JWT token.
`--jwt-signing-key`	String	The full path and filename of the key to sign a JWT. It is used by the Connection Manager for signing the JWT token.

Federated Authentication Flags

Flag	Type	Description
`--enable-oauth`	Boolean	Enables Oauth authentication. (Default=false)
`--id-provider-url`	String	Sets the identity provider URL. Example: `--id-provider-url https://provider-1234567890.id.provider.com`. This flag is required if `--enable-oauth is true`.
`--oauth-client-id`	String	Gets the Client ID from the Identity Provider. This flag is also required if `--enable-oauth` is "true".

Federated Authentication Single Sign-On Flags

Flag	Type	Description
`--fa-url`	String	Override the fhe Federated Auth Broker URL provided to the Anyware Agent. This flag can be used if auto-detection is not correcting determining the connector address. for example https://cac-vm-fqdn:port
`--enable-sso`	Boolean	Enables SSO. (Default=False)
`--sso-signing-csr-ca`	String	Path to copy intermediate CA Certificate.
`--sso-signing-csr-key`	String	Path to the intermediate key.
`--sso-signing-crl`	String	Path to a certificate revocation list.
`--sso-enrollment-url`	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-domain`	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-username`	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-password`	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-certificate-template-name`	String	Name of the certificate template that Active Directory Certification Authority Web Enrollment Service uses to sign CSR.

About Docker

The Connection Manager and Security Gateway depends on Docker 20.10.0 or higher, which must be installed on the machine before you install the Connection Manager and Security Gateway.

If you have not installed Docker yet, install it now.

If you are not sure if Docker is installed, or are not sure what Docker version you have, verify your Docker version first.

Verifying Docker Version

To verify your Docker installation and version:

1. SSH into the machine.
2. Open a console window and run the following command:

```
sudo docker -v
```

   - If Docker is *not* installed, this command will produce an error. Installation instructions are provided in the next section.
   - If you see a version number that is *lower* than 20.10.0, you must uninstall Docker and then re-install the supported version. Instructions for uninstalling and installing are provided in the next section.
   - If you see a version number that is equal to or higher than 20.10.0, you have a compatible version of Docker already installed and can skip to Connection Manager and Security Gateway installation.

Uninstalling Docker

You'll only need to do this if you have an unsupported version of Docker already on the machine. If you haven't installed Docker yet, skip this section.

To uninstall Docker:

1. SSH into the machine.
2. Open a console window and run the following command:

```
sudo dnf remove docker docker-client docker-client-latest docker-common
docker-latest docker-latest-logrotate docker-logrotate docker-engine
docker-ce docker-ce-cli containerd.io runc
```

3. When uninstalling is complete, proceed to Installing Docker.

Installing Docker

To install Docker:

If you do not have Docker installed, or if the Docker version is too low, install it using the following procedure:

1. SSH into the machine that hosts the Connection Manager and/or Security Gateway.
2. Open a console window, and run the following command. This removes the `podman` and `buildah` packages if they are installed (these packages conflict with Docker):

```
sudo dnf remove podman buildah
```

3. Run the following commands in the same console window. Note that if you copy and paste these commands into the console, you may need to press `Enter` again to execute the last command:

```
sudo dnf install -y dnf-utils
sudo dnf config-manager --add-repo https://download.docker.com/linux/
centos/docker-ce.repo
sudo dnf install docker-ce docker-ce-cli containerd.io
```

4. Confirm installation:

```
sudo docker -v
```

Installing CMSG in Offline Environments

If the Connection Manager and Security Gateway machine does not have a connection to the public internet, you must create a temporary internet-connected machine to download a pre-created offline installation bundle and then transfer the bundle to the production machine.

For information on bundle dependencies, see System Requirements.

Before You Begin

Before you proceed with installation, note the following:

- If your connection broker is configured to identify resources by host name, then DNS must be available and configured as follows:
  - Host names must be resolvable from the Connection Manager server.
  - Host names must be resolvable from the PCoIP broker.

Downloading Offline Installation Bundle

You'll need a temporary machine with internet access.

1. On the temporary machine, open a browser and go to the Connection Manager and Security Gateway download page, and download the installation bundle.
2. Transfer the installation bundle to the production machine using any acceptable method, such as a USB flash drive or SCP.

> **Note: Create Offline Bundle**
>
> If you preferred to create your own offline bundle for specific reasons, you can follow bundle creation. However, we recommend using the pre-created offline installation bundle.

Installing Connection Manager and the Security Gateway

To install the Connection Manager and the Security Gateway:

1. SSH into the production machine.
2. Navigate to the directory where you placed the installer bundle.
3. Extract the bundle and move into the newly-created `teradici-pcoip-cmsg-bundle` directory:
    - RHEL 8

      ```text
      tar xzvf pcoip-cmsg-setup_darksite-<version>.el8.tar.gz
      ```

      ```text
      cd teradici-pcoip-cmsg-bundle
      ```

    - RHEL 9

      ```text
      tar xzvf pcoip-cmsg-setup_darksite-<version>.el9.tar.gz
      ```

      ```text
      cd teradici-pcoip-cmsg-bundle
      ```

4. Run the `pcoip-cmsg-setup-offline.sh` script to complete the installation
    - **To install dependencies and follow the setup prompts to setup Connection Manager and the Security Gateway**:

      ```
      sudo ./pcoip-cmsg-setup-offline.sh
      ```

      and skip the next step.
    - **To install dependencies and run pcoip-cmsg-setup later to setup Connection Manager and the Security Gateway**:

      ```
      sudo ./pcoip-cmsg-setup-offline.sh -d
      ```

5. Move back up one directory level and then install the Connection Manager and Security Gateway:

```
cd ..
sudo pcoip-cmsg-setup install --darksite-bundle-path teradici-pcoip-cmsg-bundle <installation_flags>
```

Important: Required installation flags

There are a number of options and settings available. You can invoke the `install` command with the `--help` flag to list them:

```
pcoip-cmsg-setup install --help
```

They are also listed in the next section.

The `install` command will prompt you for required parameters that have not been supplied via flags.

Installation Flags and Options

The following flags can be used to provide values at the command line. Flags that are required are identified in the description.

Boolean values should be provided as either `true` or `false`, lowercased, as in this example:

```
--example-flag=true
```

Flag	Type	Description
`--accept-policies`	Boolean	Automatically accepts the EULA and Privacy Policy. **Required.**
`--broker-url`	String	The URL of the PCoIP Broker, specified either as a https://: or https://: or https://[]:. **Required**.
`--ca-cert`	String	The full path and filename of the custom Certificate Authority's public certificate to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--compose-file`	String	Specify the full path to a local docker-compose file.
`--darksite-bundle-path`	string	The path of darksite install bundle to be used for darksite installation
`--docker-password`	String	Password to login to private registry.
`--docker-registry`	String	Specifies the HP source for Anyware Connector images to be install from. **Debugging only**: This is intended to be used for debugging purposes and should not be used without guidance from HP support. Using this flag incorrectly can result in failed installations.
`--docker-username`	String	Username to login to private registry.
`--enable-collaboration`	Boolean	Allow multiple Anyware clients to collaborate on a Anyware agent. (Default=true)
`--enable-ipv6`	Boolean	Enables IPv6 connections (Default=false). To enable IPv6 use `--enable-ipv6=true`. To disable IPv6 use `--enable-ipv6=false`, or omit this flag.
`--external-pcoip-ip`	StringArray	Sets the public IP address of Security Gateway. If `--enable-ipv6` is true, this option may be used twice (once for IPv4 and once

Flag	Type	Description
		for IPv6). **Required if Security Gateway is enabled**
`--enable-security-gateway`	Boolean	Enable and use the Security Gateway (Default=true).
`--help`		Lists all available flags.
`--host-address`	stringArray	Sets the host FQDN/IP address. The option may be used twice (once for the IP address and once for the FQDN)
`--ignore-disk-req`	Boolean	Ignore the check for the minimum disk space requirement.
`--license-server-url`	String	The address of the locally installed License Server. Example: `https://<license-server-address>:<port>`
`--self-signed`	Boolean	Automatically generate self-signed SSL cert and key for testing purposes. If specified, `--ssl-key` and `--ssl-cert` options are ignored.
`--ssl-cert`	String	The full path and filename of the SSL certificate to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--ssl-key`	String	The full path and filename of the SSL key to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--docker-network-cidr`	Sets CIDR for Connection Manager's docker network for services. If default docker network IP range is conflict with intranet, this option should be used to solve the confliction	
`--debug`	String	Sets the log verbosity higher to help with debugging installation issues.

Flag	Type	Description
`--enable-connection-manager`	Boolean	Enable and use the Connection Manager (Default=true).
`--external-sg-ip`	StringArray	Sets public IP addresses of external Security Gateways to enable gateway failover if a Security Gateway becomes unavailable. **Only IP addresses are supported**. IP addresses should be provided in the format `--external-sg-ip=ipAddr1 --external-sg-ip=ipAddr2...`
`--jwt-verifying-cert`	String	The full path and filename of the certificate that the Security Gateway should use to validate the JWT token.
`--jwt-signing-key`	String	The full path and filename of the key to sign a JWT. It is used by the Connection Manager for signing the JWT token.

Federated Authentication Flags

Flag	Type	Description
`--enable-oauth`	Boolean	Enables Oauth authentication. (Default=false)
`--id-provider-url`	String	Sets the identity provider URL. Example: `--id-provider-url https://provider-1234567890.id.provider.com`. This flag is required if `--enable-oauth is true`.
`--oauth-client-id`	String	Gets the Client ID from the Identity Provider. This flag is also required if `--enable-oauth` is "true".

Federated Authentication Single Sign-On Flags

Flag	Type	Description
`--fa-url`	String	Override the fhe Federated Auth Broker URL provided to the Anyware Agent. This flag can be used if auto-detection is not correcting determining the connector address. for example https://cac-vm-fqdn:port
`--enable-sso`	Boolean	Enables SSO. (Default=False)
`--sso-signing-csr-ca`	String	Path to copy intermediate CA Certificate.
`--sso-signing-csr-key`	String	Path to the intermediate key.
`--sso-signing-crl`	String	Path to a certificate revocation list.
`--sso-enrollment-url`	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-domain`	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-username`	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-password`	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-certificate-template-name`	String	Name of the certificate template that Active Directory Certification Authority Web Enrollment Service uses to sign CSR.

Enabling or Disabling the Security Gateway

By default, the Security Gateway is enabled when the bundle is installed. This configuration is highly recommended for deployments where users will connect over the WAN. If your users are behind a firewall and do not access their desktops from the WAN, you may not need the Security Gateway.

If you are sure that you do not need the Security Gateway, reinstall the bundle using the `--enable-security-gateway=false` flag.

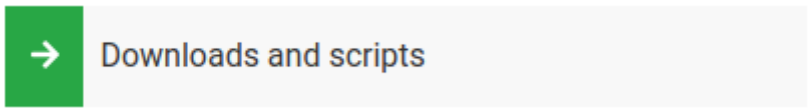
To enable the Security Gateway again, reinstall the bundle using the default options.

Creating the Installation Bundle

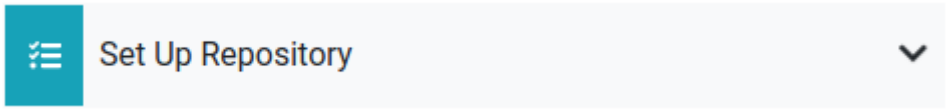
First, you'll download the package and dependencies to a temporary internet-connected machine, create an installation bundle.

To create the offline installation bundle:

1. Install Docker onto the temporary machine.
2. On the temporary, open a browser and go to the Connection Manager and Security Gateway download page.
3. Click **Downloads and scripts**:

   If you see a login button instead, click it to log into the site and then proceed.
4. Accept the End User License Agreement, then click **Set Up Repository**:

   The window will expand and show the setup scripts for each supported operating system. Copy the command for your system to the clipboard.
5. Open a console window and paste in the command you copied in the previous step. You may need to press `Enter` to execute it.

   The command fetches a configuration script from our servers and runs it locally, setting up and configuring the repository on the local machine.
6. Install **pcoip-cmsg-setup**

   ```
   sudo dnf install pcoip-cmsg-setup
   ```

7. Find and note the rpm name for the setup package. We will use this name when creating the offline bundle next.

   ```
   sudo dnf info pcoip-cmsg-setup
   ```

   The rpm name will similar to this: `pcoip-cmsg-setup-<version>-<release>`.

8. Create the offline install bundle:

```
sudo pcoip-cmsg-setup create-darksite-bundle --pcoip-cmsg-rpm-path <rpm
name>
```

...where `<rpm name>` is the name you noted in the previous step.

The process will create a tarball called `teradici-pcoip-cmsg-bundle.tar.gz`.

Once this process has completed successfully, you can dispose of the temporary machine.

Updating the Connection Manager and Security Gateway

The Connection Manager and the Security Gateway components can be installed in an offline or online deployment, depending on your environment. The procedure for updating these components is different for both scenarios.

> **Note: Load Balancer**
>
> If you have a load balancer in front of a group of Connection Manager and Security Gateway virtual machines, you can configure the load balancer to stop sending new connections to the Connection Manager and Security Gateway while you are updating.

Updating an Offline Installation

If your deployment is offline (dark site), use this procedure.

1. Download a new installation bundle .
2. Transfer the installation bundle to the production machine using any acceptable method, such as a USB flash drive or SCP.
3. Extract the bundle and move into the newly-created teradici-pcoip-cmsg-bundle directory:

    • RHEL 8

    ```
    tar xzvf pcoip-cmsg-setup_darksite-<version>.el8.tar.gz
    cd teradici-pcoip-cmsg-bundle/dependencies
    ```

    - RHEL 9

    ```
    tar xzvf pcoip-cmsg-setup_darksite-<version>.el9.tar.gz
    cd teradici-pcoip-cmsg-bundle/dependencies
    ```

4. Install the Connection Manager:

```
sudo dnf install --allowerasing pcoip-cmsg-setup*.rpm --disablerepo="*" -y
```

5. Move back up one directory level and then install the Connection Manager and Security Gateway:

```
cd ../../
sudo pcoip-cmsg-setup install --darksite-bundle-path teradici-pcoip-cmsg-
bundle <installation_flags>
```

Updating an Online Installation

To upgrade a Connection Manager and Security Gateway that can reach the public internet:

> **Important: Installation flags are required**
>
> If installation flags are absent, or are different from the original installation, the configuration on the new machine will be different.

1. Update the package:

```
dnf upgrade pcoip-cmsg-setup -y
```

2. Reinstall the package:

```
pcoip-cmsg-setup install <installation_flags>
```

To downgrade to an earlier version:

1. Downgrade the package:

```
dnf downgrade pcoip-cmsg-setup -y
```

2. Reinstall the package:

```
pcoip-cmsg-setup install <installation_flags>
```

Uninstalling Connection Manager and Security Gateway

If you want to remove the Connection Manager and Security Gateway completely from the production machine, open a console and run the following commands:

1. Close out running Docker containers:

```
sudo docker stack rm pcoipcm
sudo docker swarm leave --force
```

2. Remove Docker images

```
sudo docker rmi -f $(sudo docker images --format "{{.ID}} {{.Repository}}"
| grep -E */pcoip-cm | awk '{ print $1 }')
sudo docker rmi -f $(sudo docker images --format "{{.ID}} {{.Repository}}"
| grep -E */sg | awk '{ print $1 }')
```

3. Remove the setup files and repository information:

```
sudo dnf remove pcoip-cmsg-setup
sudo rm -f /etc/yum.repos.d/teradici-pcoip-cmsg.repo
```

4. Clean up files and directories:

```
sudo rm -rf /opt/teradici
sudo rm -rf /var/log/Teradici
```

5. Optionally remove Docker, if it will no longer be needed:

```
sudo docker system prune -f -a # remove all unused images
sudo systemctl stop docker # stop Docker
sudo systemctl disable docker # Prevent Docker from running on reboot
sudo dnf remove docker-ce docker-ce-cli containerd.io # uninstall Docker
Engine
```

6. Optionally remove the Docker repository:

```
sudo rm -f /etc/yum.repos.d/docker-ce.repo
```

Configuring

Configuring the Connection Manager and Security Gateway

You can configure the Connection Manager and/or the Security Gateway using the `pcoip-cmsg-setup configure` command.

The general syntax is:

```
sudo pcoip-cmsg-setup configure <flags>
```

For example, to specify a broker url, you would open a console window and enter the following:

```
sudo pcoip-cmsg-setup configure --broker-url https://<example>
```

Configuration Flags and Options

The following flags can be used to provide values at the command line.

Flag	Type	Description
`--broker-url`	String	The URL of the PCoIP Broker, specified either as a https://: or https://: or https://[]:. **Required**.
`--clear-host-address`	Boolean	Clears the host address.
`--ca-cert`	String	The full path and filename of the custom Certificate Authority's public certificate to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--clear-trusted-license`	Boolean	Clears trusted license certificate and key.
`--compose-file`	String	Specify the full path to a local docker-compose file.
`--docker-password`	String	Password to login to private registry.
`--docker-registry`	String	Specifies the HP source for Anyware Connector images to be install from. **Debugging only**: This is intended to be used for debugging purposes and should not be used without guidance from HP support. Using this flag incorrectly can result in failed installations.
`--docker-username`	String	Username to login to private registry.
`--enable-collaboration`	Boolean	Allow multiple Anyware clients to collaborate on a Anyware agent. (default true)
`--external-pcoip-ip`	StringArray	Sets the public IP addresses of VM which hosts Security Gateway. This option can be used twice, once for IPv4 and once for IPv6 (if using). **Required if Security Gateway is enabled**.
`--help`		Display configuration help.
`--host-address`	stringArray	Sets the host FQDN/IP address. The option may be used twice (once for the IP address and once for the FQDN)
`--license-server-url`	String	The address of the locally installed License Server. Example: `https://<license-server-address>:<port>`
`--ssl-cert`	String	The full path and filename of the SSL certificate to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--ssl-key`	String	

Flag	Type	Description
		The full path and filename of the SSL key to be used in the Connection Manager and Security Gateway. **Required if `--self-signed` is not used.**
`--trusted-license-cert`	String	Trusted Customer License certificate path. Defaults to `/opt/teradici/pcoipcm_data/certs/tcl-cert.crt`).
`--trusted-license-cert-key`	String	Trusted Customer License certificate key path. Defaults to `/opt/teradici/pcoipcm_data/certs/tcl-cert.key`.
`--docker-network-cidr`	String	Sets CIDR for Connection Manager's docker network for services.
`--enable-horizon`	Boolean	Enables/Disables HP Anyware to be brokered with VMware Horizon (Default=false).
`--external-sg-ip`	StringArray	Sets public IP addresses of external Security Gateways to enable gateway failover if a Security Gateway becomes unavailable. IP address should be provided in the format `--external-sg-ip=ipAddr1 --external-sg-ip=ipAddr2...`
`--jwt-verifying-cert`	String	The full path and filename of the certificate that the Security Gateway should use to validate the JWT token.
`--jwt-signing-key`	String	The full path and filename of the key to sign a JWT. It is used by the Connection Manager for signing the JWT token.

Federated Authentication Flags

Flag	Type	Description
`--enable-oauth`	Boolean	Enables Oauth authentication. (Default=False)
`--id-provider-url`	String	Sets the identity provider URL. Example: `--id-provider-url https://provider-1234567890.id.provider.com`. This flag is required if `--enable-oauth is true`.
`--oauth-client-id`	String	Gets the Client ID from the Identity Provider. This flag is also required if `--enable-oauth` is "true".

Federated Authentication Single Sign-On Flags

Flag	Type	Description
`--fa-url`	String	Override the fhe Federated Auth Broker URL provided to the Anyware Agent. This flag can be used if auto-detection is not correcting determining the connector address. for example https://cac-vm-fqdn:port
`--enable-sso`	Boolean	Enables SSO. (Default=False)
`--sso-signing-csr-ca`	String	Path to copy intermediate CA Certificate.
`--sso-signing-csr-key`	String	Path to the intermediate key.
`--sso-signing-crl`	String	Path to a certificate revocation list.
`--sso-enrollment-url`	String	Gets the URL to the Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-domain`	String	Domain of the user to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-username`	String	Username for accessing Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-password`	String	Password for the username to access Active Directory Certification Authority Web Enrollment Service.
`--sso-enrollment-certificate-template-name`	String	Name of the certificate template that Active Directory Certification Authority Web Enrollment Service uses to sign CSR.

Configuring Failover Security Gateways

You can set up additional failover Security Gateways to ensure uninterrupted connectivity. In failover Security Gateway deployments, if the gateway used to establish a PCoIP session becomes unavailable, the session is automatically transferred to the next available gateway configured for this purpose. This ensures continuity of the session in the event of hardware failures or network disruptions.

Failover gateways can be set up at the time of installing the Connection Manager and/or the Security Gateway. They can also be configured later, following the steps described below.

> **Info**
>
> Before you begin, make sure you have the IP addresses of the gateways handy. At this time, only **IP addresses** can be specified.

1. On the machine where the Connection Manager and/or the Security Gateway is installed, open a Terminal.
2. Run the following command:

```
sudo pcoip-cmsg-setup configure --external-sg-ip=IPAddress1 --external-sg-ip=IPAddress2
```

where,

3. `--external-sg-ip`: The flag that sets public IP addresses of external Security Gateways to enable gateway failover. **Only IP addresses** are supported.
4. IPAddress1, IPAddress2: Represents the IP addresses of the security gateways that will handle failover scenarios.

Security and Certificates

Security Considerations

All certificate files must be in base64-encoded PEM format.

Follow your organization's security policy

For all security and certificate procedures, ensure that you follow your organization's security policy.

Note: Securing Connection Manager and Security Gateway

Connection Manager and Security Gateway are critical components that enable end-users to authenticate and connect to their remote desktops. We recommend that the Connection Manager and Security Gateway are appropriately secured, and access to them is limited to authorized systems and users only.

Creating, Installing, and Managing Certificates

In order to establish secure TLS connections with clients, certificates must be configured for the Connection Manager and the Security Gateway. If the required certificate files are not present or they are improperly configured, clients will not be able to connect and users will not be able to establish PCoIP sessions.

Only certificates with RSA private keys having at least 2,048-bit length are supported. RSA private keys having at least 3,072-bit length are recommended. Certificates with DSA private keys are not supported. Certificates that include an MD5-based digital signature algorithm are not supported.

Both the Connection Manager and Security Gateway support wildcard certificates which can be used on multiple Connection Manager and Security Gateway servers.

If you are ready to replace your default self-signed certificates with your own signed certificates, proceed to Signed Certificates for Production.

Ensure all certificate files follow your security policy

Protect the regenerated certificate and ensure all certificate files you use conform to your organization's security policy.

Default Certificate

The Connection Manager and Security Gateway installation script generates a self-signed certificate during installation to facilitate testing. **This should be replaced with your own certificate, signed by a trusted Certificate Authority (CA), when deploying a production system**.

By default, both the Connection Manager and the Security Gateway use the same private key and signed certificate; if your security policy requires it, each service can use its own key/certificate pair instead. If two sets of certificates are required, follow these procedures twice to generate two key/certificate pairs and configure the Security Gateway appropriately.

Copying certificates from a Window system to a Linux system

When copying certificates from a Windows system to a Linux system, line endings might be incorrect. Check that the certificate text is formatted correctly.